8. 4. The ElGamal Digital Signature

Define \( GF(p) = F_p \)

**System public key:** \( p \) is a prime such that the discrete log problem in \( F_p \) is infeasible, \( \alpha \in F_p^* \), a primitive element in \( F_p \).

**User Bob:** Selects \( x, 0 < x < p \) with \( (x, p-1) = 1 \) as his private key. Compute \( y = \alpha^x \) as his public key.
**Signing process:** To sign a message $m$ (in the following, we always suppose $m$ is a hashed value of the message $m$.)

(a) Randomly picks $k$, $0 < k < p$ with $(k, p-1) = 1$.

(b) Computes $r = \alpha^k$

(c) Solve for $s$ in the equation:

$$m = xr + ks \mod p - 1$$

(called the signing equation)

i.e, $s = k^{-1} (m - xr) \mod p - 1$

Then, $(r, s)$ is a digital signature of $m$. 

$(m, (r, s))$ as a signed message

**Verifying process:** Check whether

$$\alpha^m = y^r r^s$$

(i.e, $\alpha^{s^{-1}m} y^{-rs^{-1}} = r$)
ElGamal and DSS Signing Process

Message \( m \) \rightarrow \text{Hash} \rightarrow \text{Sign} \rightarrow (r, s) \rightarrow \text{signature}

- \( x \): private key
- \( k \): secret number per message

\[ \alpha^x r = \alpha^k \]
ElGamal and DSS Verifying Process

\[ m \rightarrow \text{Hash} \rightarrow \text{Verifying} \]

\[ y = \alpha^x: \text{public key} \]
Security of the ElGamal Signature Scheme:

Consider

\[ m = xr + ks \mod p - 1 \quad (1) \]

If the attacker can compute \( y = \alpha^x \) to obtain \( x \), then he can forge any signature since in (1) he can pick \( k \) to compute \( r \), and therefore, obtain \( s \).

Thus the security of the ElGamal digital signature algorithm is based on the difficulty of solving discrete log problem in \( F_p \).

**Remark:** The random number \( k \) should be different per message.
Example 1. System parameters: \( p = 23 \), \((p-1)=2\times11\) then \( \alpha = 5 \)

primitive in \( \mathbb{Z}_{23} \)

User Bob: Private key: \( x = 3 \)

Public-key: \( y = 5^3 \mod 23 = 10 \)

Signing Process:

Message \( m = 7 \) (We assume that this is the hashed value for simplicity, i.e., \( h(m) = 7 \).)

(a) Pick a random number \( k = 9 \)

(b) Compute \( r = \alpha^9 = 5^9 = 11 \mod 23 \)

(c) Solving for \( s \) in the equation: \( m = xr + ks \mod p-1 \)

\[
s = k^{-1}(m - xr) = -5(7 - 3\times11) = -2 \mod 22
\]

Signature: \((r, s) = (11, 20)\)
Verifying process: Check whether

\[ \alpha^m = y^r r^s \]

Compute:

\[ \alpha^m = 5^7 = 17 \quad \text{and} \quad y^r r^s = 10^{11} 11^{20} = 22 \times 6 = 17 \]

Thus, \((11, 20)\) is a valid signature of \(m = 7\).